Stockholms stad

Handbok Informationsklassificering

Stockholm
2008-03-18

1. Informationssäkerhet

Kraven på säkerhet i en organisation med IT-stöd skall ställas i relation till de krav som ställs på organisationens verksamhet i övrigt.

1.1 Definitioner

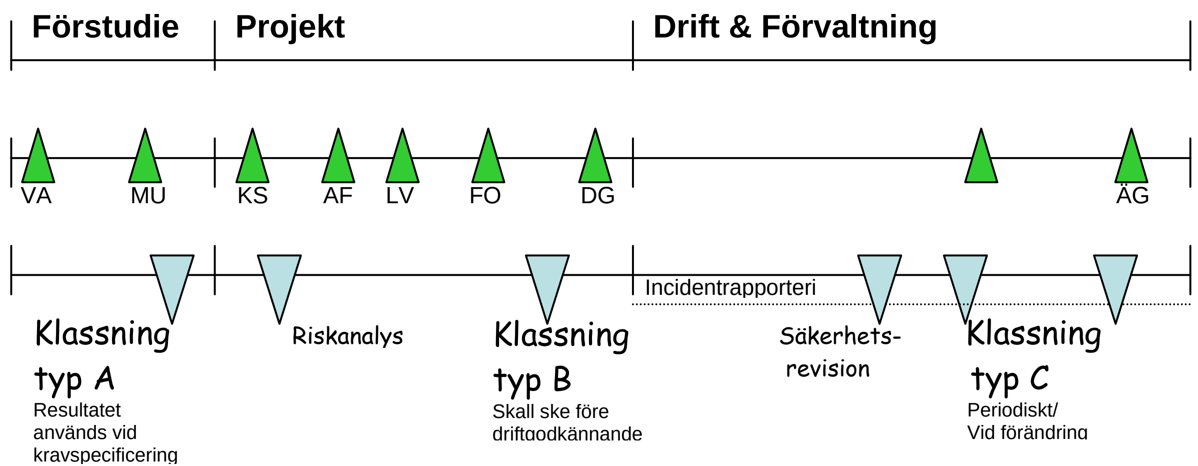
Begrepp	Beskrivning
Policy	Anger ledningens viljeinriktning och stöd för informationssäkerhet. Policyn beskriver ”att något ska finnas”.
Riktlinjer	Anger VAD som skall göras för att uppfylla de övergripande målen i policyn.
Anvisningar	Anger på en funktionell nivå HUR (på vilket sätt) skyddsåtgärder och administrativa processer skall utformas.
Instruktioner	Ges för specifika IT-system/e-tjänster och/eller anvisningar. Instruktioner beskriver "hur och av vem" anvisningarna ska införas/följas.
Användare	Individ som utnyttjar informationstillgångar.
Autenticering	Verifiering av uppgiven identitet.
Avbrottsplan [IT]	Plan för att kunna återuppta driften efter driftstörning eller då IT-system/e-tjänst inte fungerar som avsett. Avbrottsplanen baseras på vad som beskrivs i kontinuitetsplanen.
Behörighets-KontrollSystem (BKS)	Säkerhetsfunktioner som tillsammans kontrollerar och registrerar användarens aktiviteter i ett system eller en e-tjänst. BKS omfattar tre grundläggande säkerhetsfunktioner. Dessa skall tillsammans tillse att verksamhetens säkerhetsregler efterlevs: a) identifiering av användaren och verifiering av den föregivna identiteten (se identitet samt autenticering) b) reglering av åtkomsträttigheter c) registrering av användarens aktiviteter i systemet/e-tjänsten (se logg).
Hot	Möjlig, oönskad händelse med negativa konsekvenser för verksamheten.
Identitet	Unik beteckning för en viss individ.
Incident	Säkerhetshändelse som kan/kunnat få/har fått allvarliga konsekvenser för verksamheten.
Informations-klassificering	Ett formellt sätt att fastställa rätt skyddsnivå för ett IT-system eller en e-tjänst. Uttrycks i en s.k. säkerhetsprofil**.**
Informations-säkerhet	Säkerhet beträffande informationstillgångar avseende förmågan att upprätt-hålla erforderlig åtkomstbegränsning, riktighet, tillgänglighet och spårbarhet.

Informations-tillgångar	En organisations informationsrelaterade tillgångar, vilka har ett värde för organisationen och därmed är skyddsvärda. *Exempel på informationstillgångar är:* • *Information (databaser, metodik, dokument, etc.)* • *Program (tillämpningar, e-tjänster, operativsystem, etc.)* • *Tjänster (nätförbindelser, abonnemang, etc.)* • *Fysiska tillgångar (datorer, datamedia, lokala nätverk, etc.)*
IT-system	Är en konstellation av datorer, in- och utmatningsutrustning, minnesenheter, program, kommunikationsutrustningar, metoder och procedurer organiserade med uppgift att genomföra elektronisk behandling av information i syfte att tillgodose ett uttalat behov.
Kontinuitetsplan [för verksamheten]	Dokument som beskriver hur verksamheten skall bedrivas när identifierade, kritiska verksamhetsprocesser allvarligt påverkas under en längre, specificerad tidsperiod.
Logg	Insamlad information om de operationer som utförs i ett IT-system/e-tjänst. Tre typer av loggar är aktuella: transaktionslogg, driftlogg och säkerhetslogg.
Riktighet	Egenskap att information inte obehörigen, av misstag eller på grund av funktionsstörning har förändrats.
Risk	Produkten av sannolikheten för att ett givet hot realiseras och de konsekvenser hotet medför.
Riskanalys	Process som identifierar säkerhetsrisker, bestämmer deras betydelse och föreslår skyddsåtgärder. Möjlighet finns till beräkning av uppkommande skadekostnad.
Åtkomstbegräns-ning (Sekretess)	Avsikten att innehållet i ett informationsobjekt (eller ibland även dess existens) inte får göras tillgängligt eller avslöjas för obehöriga.
Service Level Agreement (SLA)	Dokument som reglerar vad som överenskommits mellan objektansvarig/-representant och IT-chef gällande drift och förvaltning av visst IT-system/e-tjänst.
Spårbarhet	Möjlighet att entydigt kunna härleda utförda aktiviteter i IT-systemet/e-tjänsten till en identifierad användare. För att åstadkomma spårbarhet krävs åtminstone identifiering och autenticering av användare samt loggning av relevanta händelser i IT-systemet/e-tjänsten.
Sårbarhet	Brist i skyddet av en tillgång exponerad för hot.
Säkerhet	Egenskap eller tillstånd som innebär skydd mot risk i samband med insyn, förlust eller påverkan; oftast i samband med medvetna försök att utnyttja eventuella svagheter.
Säkerhetsprofil	Alla IT-system/e-tjänster har ett skyddsbehov. Skyddsbehovet varierar beroende på typ av informationstillgång. Genom att klassificera informationen

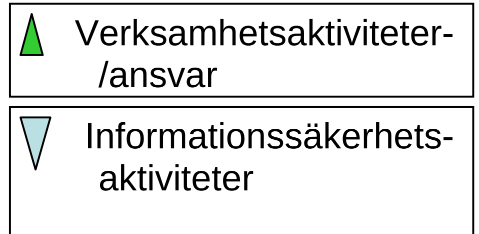
	med avseende på åtkomstbegränsning, riktighet, tillgänglighet och spårbarhet erhålls en säkerhetsprofil. Denna avgör vilka säkerhetskrav som ställs på informationstillgången.
Tillgänglighet	Möjligheten att utnyttja informationstillgångar efter behov i förväntad utsträckning och inom önskad tid.
Tillgänglighets-avtal	Se **Service Level Agreement (SLA)** ovan.
Åtkomst-/behörighets-kontroll	Syftar till att reglera och kontrollera en användares åtkomst till olika informationstillgångar samt att skydda information och program, så att de endast är tillgängliga utifrån tilldelad (roll-)behörighet.

1.2 Livscykel IT-system/e-tjänst

Nedanstående figur beskriver hur informationssäkerhetsaktiviteter påverkar ett IT-system/e-tjänst under hela dess livscykel.



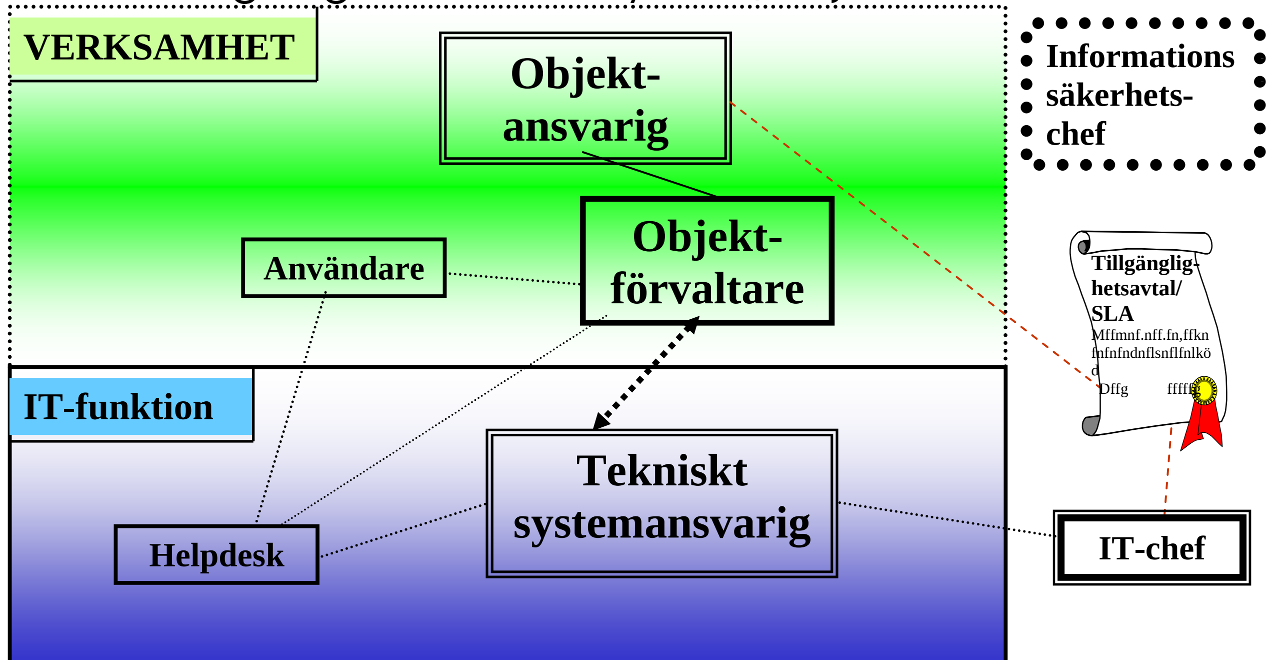
Förkortningar:
VA=Verksamhetsanalys, MU=Marknadsundersökning,
KS=Kravspecifikation, AF=Anbudsförfrågan,
LV=Leverantörsval, FO=Förvaltningsorganisation,
DG=Driftgodkännande, ÄG=Ändringsgodkännande



1.3 Roller och ansvar

Nedanstående figur visar de viktigaste rollerna i samband med förvaltning av IT-system/e-tjänster.

Förvaltningsorganisation IT-system/e-tjänst



OBJEKTANSVARIG: Har det övergripande ansvaret för systemet/e-tjänsten inom de ramar för normer, policy och resurser som tilldelats av samordnande (överordnad) instans. Ansvaret omfattar även funktionalitet, ekonomi och säkerhet.
Delegering kan ske till **OBJEKTANSVARIGREPRESENTANT**.

OBJEKTFÖRVALTARE: Har till arbetsuppgift att kontinuerligt bevaka systemet/e-tjänsten, dess egna data och dokumentation, initiera nödvändiga förändringar och tillse att för handhavandet nödvändiga beslut fattas. Handhar även systemet/e-tjänstens behörigheter.
Utses av objektansvarig.

TEKNISKT SYSTEMANSVARIG: Ansvarar för att systemet/e-tjänsten drivs enligt vad som överenskommits mellan parterna.

OBS! För begreppen **Objektförvaltare** och **Tekniskt systemansvarig** kan olika benämningar förekomma inom stadens förvaltningar och bolag.

1.4 Klassificering av information

1.4.1 Riktlinjer för informationsklassificering

Enligt stadens regelverk för Informationssäkerhet skall informationstillgångar klassificeras (värderas) så att rätt skyddsnivå etableras för stadens IT-system/e-tjänster.

Anvisningar

1.4.1.1 *Anvisningar för Informationsklassificering*

Pos	Text
Allmänt	***Mål*** ***Att säkerställa att informationssäkerhet byggs in i IT-system/e-tjänster från början och att informationssäkerheten upprätthålls.*** Information som skapas, inhämtas, distribueras, bearbetas och lagras i stadens IT-system är en av dess viktigaste tillgångar. Syftet med att klassificera informationstillgångar är att säkerställa att de ges ett tillräckligt skydd. Att klassificera information är en grundläggande aktivitet för att särskilja den information som på ett eller annat sätt ställer högre krav på säkerhet. Förutom legala krav på skydd (främst personrelaterad information) skall verksamhetens bedömning av informationens värde avseende åtkomstbegränsning, riktighet, tillgänglighet och spårbarhet avgöra omfattningen av det skydd som skall uppnås. Obs! e-tjänst där ingen förändring av informationens värde sker behöver inte klassificeras eftersom skyddsbehovet förblir oförändrat. ***Vad innebär klassificering?*** ***Klassificering är ett formellt sätt att, ur ett verksamhetsperspektiv, fastställa lämplig skyddsnivå för ett IT-system eller en e-tjänst. Uttrycks i en säkerhetsprofil.*** Följande aktiviteter ingår vid klassificering av ett IT-system/e-tjänst (Pkt 1-4 dokumenteras i ett Protokoll, Pkt 6 men ej pkt 7-8 gäller blivande IT-system/e-tjänster i samband med kravspecificering, pkt 7-8 men ej pkt 6 i övriga fall): ***1***. *Beskrivning av IT-systemet/e-tjänsten och eventuella systemsamband* ***2***. *Identifiera IT-systemet/e-tjänstens projekt-/förvaltningsorganisation* ***3***. *Identifiera och verifiera legala krav på IT-systemet/e-tjänsten* ***4***. *Fastställande av säkerhetsprofil* Säkerhetskrav avseende **åtkomstbegränsning, riktighet, tillgänglighet** och **spårbarhet** avgörs genom värdering av dessa begrepp med hjälp av en mall. Värderingen, för vart och ett av begreppen, görs via en tregradig skala där nivå 1 är högsta och nivå 3 lägsta säkerhetsnivå och resulterar i en säkerhetsprofil: –Nivån för **åtkomstbegränsning** fastställs utifrån bedömning av den skada som uppstår om känslig information i IT-systemet/e-tjänsten kommer i orätta händer

–Nivån för **riktighet** fastställs utifrån bedömning av den skada som uppstår om information i IT-systemet/e-tjänsten är oriktig
–Nivån för **tillgänglighet** fastställs utifrån verksamhetens tillgänglighetskrav på IT-systemet/e-tjänsten
–Nivån för **spårbarhet** fastställs utifrån möjligheten att entydigt kunna härleda utförda aktiviteter i systemet/e-tjänsten till en identifierad användare.

5. *Utifrån säkerhetsprofilen, med hjälp av en Kravkatalog, fastställa aktuella säkerhetskrav*

6. *Framtagande av Kravspecifikation IT och Säkerhet*

7. *Verifiera att IT-systemet/e-tjänsten har den skyddsnivå som säkerhetsprofilen anger – annars är ett bristläge ur säkerhetssynpunkt identifierat*

8. *Eventuella brister förtecknas och prioriteras för åtgärd.*

När görs klassificering?

För IT-system/e-tjänster vid följande tidpunkter:

1. *Under förstudie/projektfasen:*

a) på det blivande IT-systemet/e-tjänsten i samband med funktionell krav-specificering (Typ A)
b) på det blivande IT-systemet/e-tjänsten innan driftgodkännande (Typ B)

2. *För IT-system/e-tjänster i drift:*

a) periodiskt, dock minst vartannat år (Typ C)
b) vid större förändring i IT-systemet/e-tjänsten (Typ C)

Beställare/projektledare/objektansvarig ansvarar för att klassificering sker och tidsåtgången är ca 4-7 timmar plus eventuellt uppföljningsmöte.

Deltagare under pkt 1 är:
Beställare/projektledare, projekt- och blivande förvaltningspersonal, egen IT-ansvarig, representant/er från IT-avdelningen samt informationssäkerhetssamordnare.

OBS! Vid anskaffning av IT-system/e-tjänster är det viktigt att IT-avdelningens representant även medverkar vid utvärderingen av inkomna anbud så att de IT-tekniska kraven beaktas på bästa sätt.

Deltagare under pkt 2 är:
Objektansvarig/-representant, objektförvaltare, användare, egen IT-ansvarig, tekniskt systemansvarig samt informationssäkerhetssamordnare.

Klassificeringen bör genomföras av en person med erfarenhet från både IT-verksamhet och informationssäkerhetsarbete. Det är även viktigt att denne person uppfattas som neutral av de parter som medverkar vid klassificeringen.

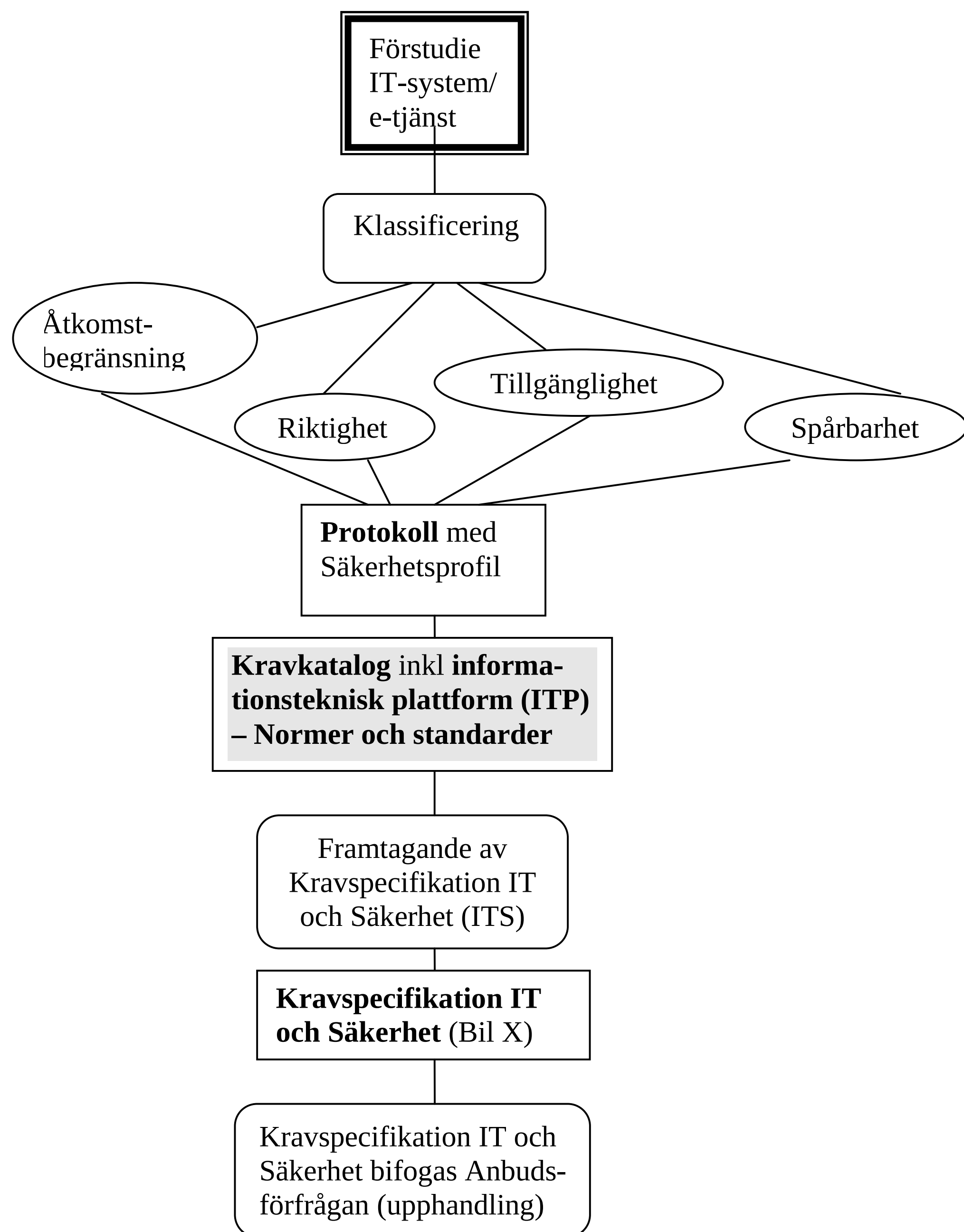
Dokumentation

Protokollet

Resultatet av en klassificering dokumenteras i ett Protokoll med tillhörande bilagor. Originalet förvaras hos beställare/objektansvarig och en kopia tillställs stadens informationssäkerhetschef.

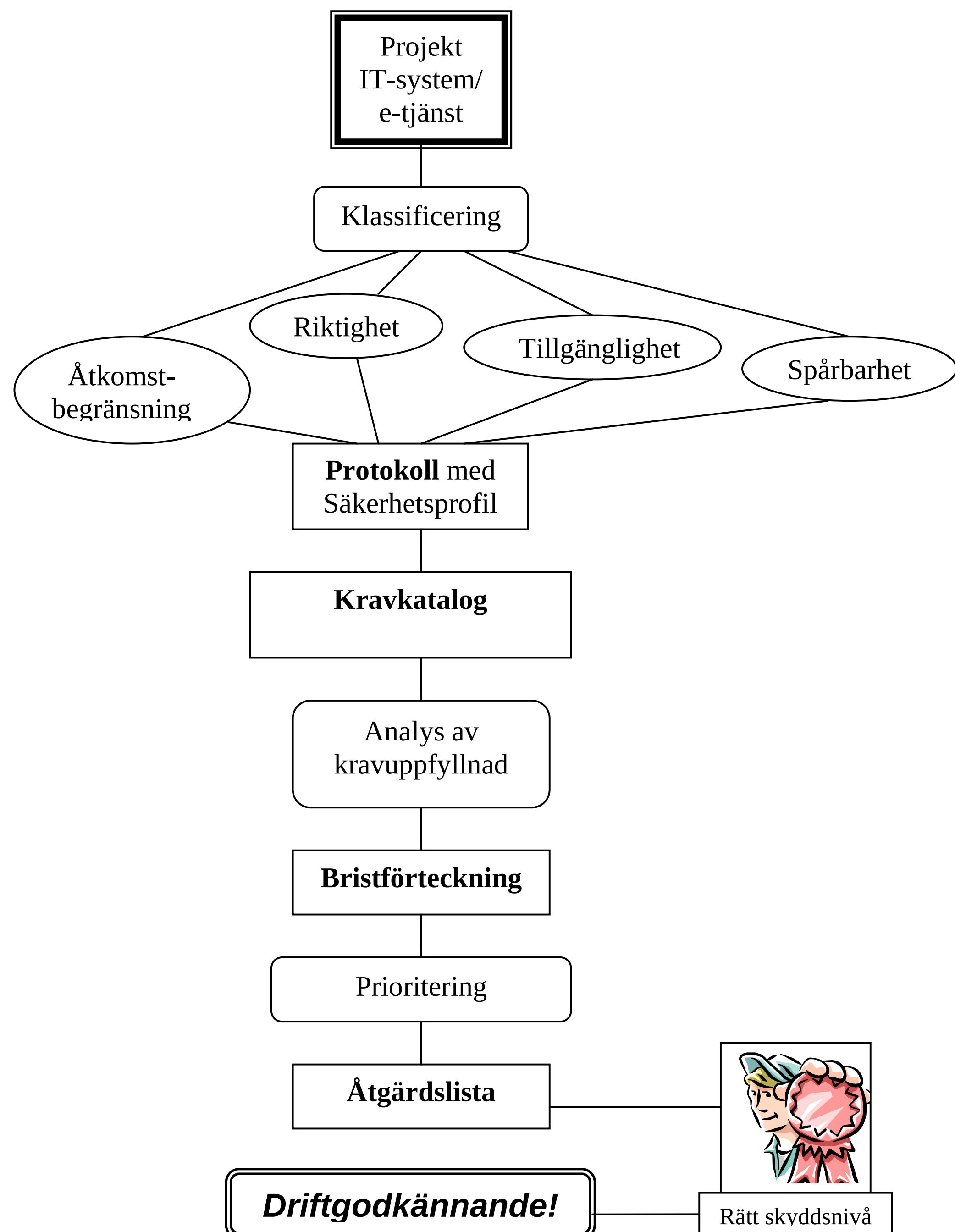
1.4.1.1.1 **Anvisning klassificering Typ A**

Klassning sker i samband med framtagandet av den funktionella kravspecifikation som ingår i Anbudsförfrågan. Resultatet av klassningen är en 'Kravspecifikation IT och säkerhet' där, för systemet/e-tjänsten, aktuella IT- och säkerhetskrav framgår. Dessa bifogas den funktionella kravspecifikationen.

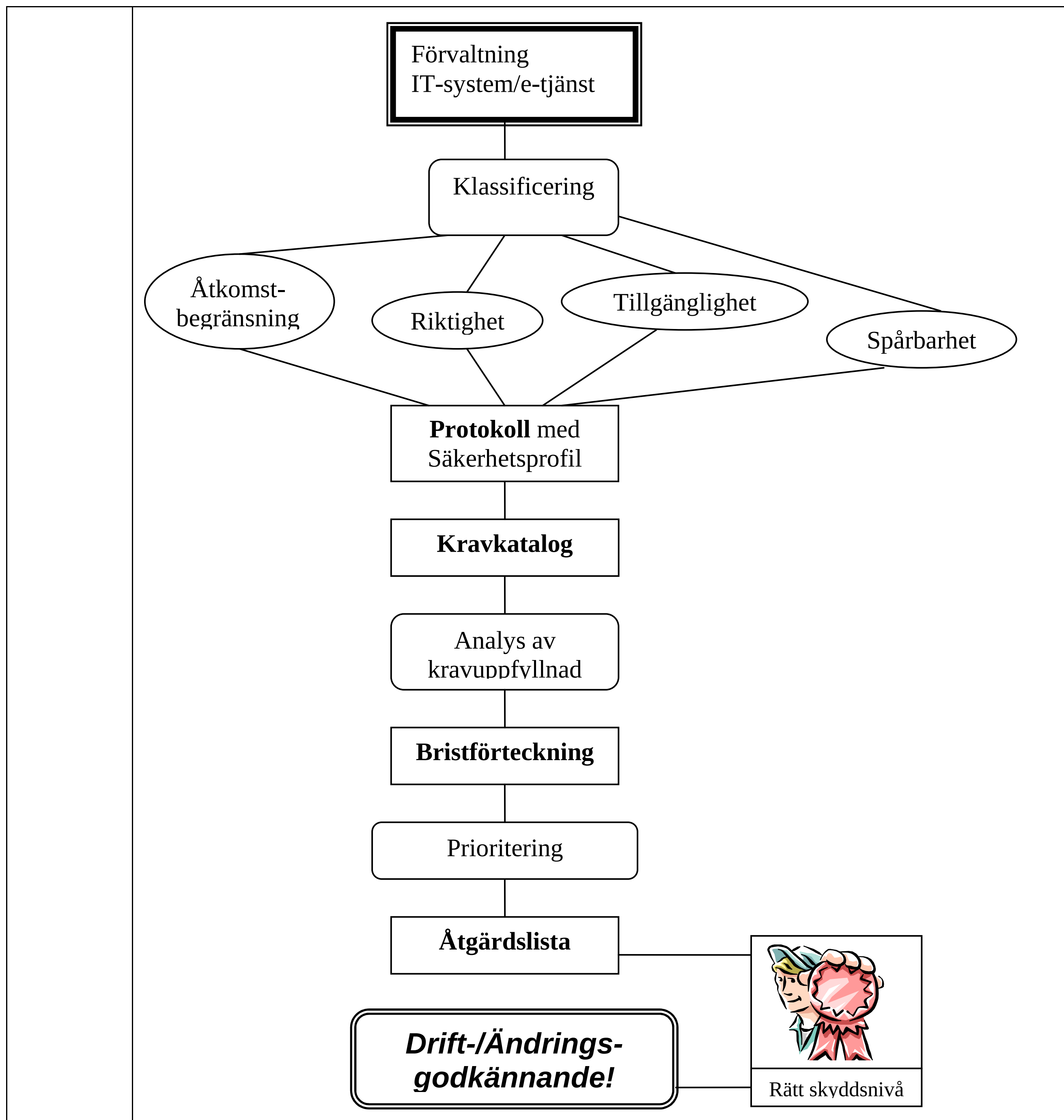


1.4.1.1.2 **Anvisning klassificering Typ B**

Klassning sker innan Driftgodkännande av det nya IT-systemet/e-tjänsten. Syftet är att verifiera den tidigare fastställda Säkerhetsprofilen och att från resultatet kontrollera om samtliga aktuella krav är uppfyllda. Om så är fallet kan systemet/e-tjänsten, ur informationssäkerhetssynpunkt, driftgodkännas.



1.4.1.1.3	**Anvisning klassificering Typ C** System som är i driftläge påverkas förr eller senare av oliks slags för-ändringar av vilka vissa kan ge upphov till förändrad funktionalitet. Detta kan påverka Säkerhetsprofilen och härigenom förändra kravbilden på systemet/e-tjänsten. Innan uppdateringarna införs skall klassificering ske. Även utan förändringar påverkas regler och rutiner av ’tidens tand’ så att tidigare fastställd kravbild inte längre är helt uppfylld. Av detta skäl skall klassificering regelbundet ske med 2-3 års intervall.


Förvaltning
IT-system/e-tjänst
Klassificering
Åtkomst-
begränsning
Riktighet
Tillgänglighet
Spårbarhet
Protokoll med
Säkerhetsprofil
Kravkatalog
Analys av
kravuppfyllnad
Bristförteckning
Prioritering
Åtgärdslista
Drift-/Ändrings-
godkännande!
Rätt skyddsnivå

1.4.2 Protokoll

Klassificeringen genomförs under ledning av en oberoende klassificeringsledare där verksamhets- och IT-representanter går igenom de olika punkterna i Protokollet (bil 1) och där resultatet dokumenteras av klassificeringsledaren.
I protokollet fastställs tillämpliga legala krav.
Här fastställs även den s.k Säkerhetsprofilen och till hjälp används en mall 'Anvisningar för klassificering av IT-system' (bil 2A) alt. 'Anvisningar för klassificering av e-tjänster' (bil 2B).

1.4.3 Kravkatalog

Utifrån den fastställda Säkerhetsprofilen och typ av klassning (Typ A, B eller C) ställs ett antal, av staden definierade, säkerhetsrelaterade krav på IT-systemet/e-tjänsten. Ju högre vikt (3 nivåer finns där nivå 3 är grundnivåkrav) som satts på begreppen åtkomstbegränsning, riktighet, tillgänglighet och spårbarhet ju fler krav ställs på systemet/e-tjänsten.
I Kravkatalogen (bil 3A, 3BC) är kraven grupperade nivåvis per begrepp.
Kravkatalogen finns i två utgåvor. För klassificeringar Typ A (se pkt 1.4.5 nedan) skall bilaga 3A användas och endast de krav som inte är gråmarkerade är aktuella. I övriga fall är bilaga 3BC aktuell (se pkt 1.4.6 nedan).

1.4.4 Informationsteknisk plattform (ITP) - Normer och standarder

Förutom de krav som skall uppfyllas enligt Kravkatalogen är det viktigt att hänsyn tas till den informationstekniska miljön i vilken stadens IT-system/e-tjänster driftas.
Vid upphandling/anskaffning av nya IT-system/e-tjänster måste de informationstekniska kraven beaktas innan driftgodkännande kan ske. I dokumentet 'Informationsteknisk plattform - Normer och standarder' (bil 4) återfinns vad som gäller för staden.

1.4.5 Kravspecifikation IT och Säkerhet (Klassificering Typ A)

I samband med upphandling/anskaffning av ett IT-system/e-tjänst produceras en funktionell kravspecifikation. Som en bilaga till denna skall 'Kravspecifikation IT och Säkerhet' (bil 5) finnas.
Härigenom lämnas ett underlag till anbudslämnare vilket beskriver samtliga de krav (funktionella, legala, informationstekniska och säkerhetsmässiga) som staden ställer.
Denna kompletta kravbild underlättar även vid utvärdering av inkomna anbud.
Dokumentet är uppdelat i två delar där den första delen (K1), på grundnivå, beskriver de informationstekniska kraven. IT-avdelningen är ansvarig för innehållet med anpassning till vad upphandlingen avser.
Den andra delen (K2) redovisar de systemspecifika kraven från klassningen, härledda från både Protokollet och Kravkatalogen.
Verksamhetsrepresentanter ansvarar för innehållet i denna del.

1.4.6 Bristförteckning och Åtgärdslista (Klassificering Typ B och C)

Utifrån den säkerhetsprofil som fastställs vid klassificeringen görs en avstämning mot aktuella krav i Kravkatalogen. I de fall kraven inte är uppfyllda noteras de i en Bristförteckning (bil 6) och nyttan av att bristen undanröjs bedöms (prioritering).
För att undanröja en brist kan en eller flera åtgärder vidtas. Dessa noteras i en Åtgärdslista (bil 7) där åtgärden beskrivs, vem som är ansvarig och när bristen beräknas vara avhjälpt.

När bristerna är åtgärdade uppfyller systemet/e-tjänsten stadens krav gällande informationssäkerhet.